SFA Post Deployment Maintenance Approach

SFA Modernization Program

US Department of Education

Table Of Contents

1 Introduction

1.1 Purpose

The SFA modernization program will help SFA architect, design and deploy numerous systems as SFA strives to implement the modernization blueprint. A key component to the success of such a venture will be how well SFA is able to support its present and future systems. This document seeks to provide a means for SFA to reliably sustain those systems.

SFA has been supporting a variety of users, multiple systems and vendor relationships for some time. In doing so, vendor/contractor support teams have developed a set of practices to manage post deployment activities. These internal SFA practices should be analyzed and if possible utilized going forward. To that end, this document does not suggest a start from scratch approach is needed. In fact, the document defines an approach that supplements the effective practices SFA has in place with Andersen Consulting best practices and lessons learned.

The purpose of this document is to define a best practice approach for SFA to support the maintenance phase of a business capability deployed as part of the SFA Modernization Blueprint's implementation. The approach is composed of the functions, organization and procedures that are required to be able to efficiently operate, maintain, and upgrade the applications that are delivered by the SFA Modernization Program. Most importantly, this approach will define a lasting process. As time passes, continuous improvements will become an integral part to help ensure the success of the program.

1.2 Scope

The objective of the maintenance phase is to operate the new business capabilities that were created and deployed in the previous phase (deployment) of the system development life cycle. The work in this phase must meet the formal service targets and metrics established earlier (during the capability analysis and deployment phases). In addition, it must provide feedback for improvements based on measurements of actual performance against those targets. Given these guidelines, the post deployment maintenance approach should apply to all information systems and related system engineering activities associated with a deployed business capability. This would include hardware, custom off the shelf (COTS) and/or custom software, and documentation. In particular, the focus of this document is on the enterprise perspective of maintenance and support.

Note, the following chart depicts the categories and functions of activity this approach targets.

Post Deployment Targeted Areas

Service Management	***Systems Management***	***Service Planning***	***Managing Change***
Service Level Agreement (SLA) Management	***Production Control***	***Service Management Planning***	***Controlling***
- SLA Definition	*- Production Scheduling*	*- Service Costing and Pricing*	*- Change Control*
- SLA Reporting	*- Print Management*	*- Training Planning*	***- Asset Management***
- SLA Control	*- File Transfer and Control*		*- Rollout Management*
- SLA Review	*- System Stamp and Shutdown*	***Systems Management Planning***	*- Release Control*
	- Mass Storage Management	*- Physical Site Planning*	*- Migration Control*
Operating Level Agreement (OLA) Management	*- Backup/Restore Management*	***Security Planning***	***- License Management***
- OLA Definition	*- Archiving*	*- Capacity Modeling and Planning*	
- OLA Reporting		*- Contingency Planning*	***Testing***
- OLA Control	***Monitoring***	*- Disaster Recovery Planning*	*- Product Validation*
- OLA Review	*- Event Management*	*- Hardware Maintenance Planning*	*- Release Testing*
	- Performance Management		
Customer Service (i.e. Help Desk)	*- Physical Site Management*	***Managing Change Planning***	***Implementing***
- Incident Management		*- Rollout Planning*	*- Procurement*
- Problem Management	***Failure Control***	*- Release Planning*	*- Initial Installation*
- Request Management	*- Fault Management*	*- Procurement Planning*	*- System Component Configuration*
	- Recovery		*- Software and Data Distribution*
Quality Management	*- Disaster Recovery*	***Strategic Planning***	***- User Administration***
Quality Management	*- Hardware Maintenance*		
Training			
	Security Management		
Administration			

- *Billing and Accounting*			
- *Contract Management*			

Current State of Post Deployment Maintenance

SFA currently conducts post deployment maintenance in the following ways: the infrastructure components are upgraded and supported by the virtual data center and legacy contractor organizations on an as needed basis. Mainframe and system software updates (problem fixes, upgrades, enhancements) are controlled by the legacy contractor(s) operating those systems and the virtual data center in Meriden. An SFA contracting office technical representative (COTR) for the virtual data center is responsible for acquisition/procurement tasks. The legacy contractors for the production systems and virtual data center representatives send requests for support (equipment and personnel) to the respective COTR.

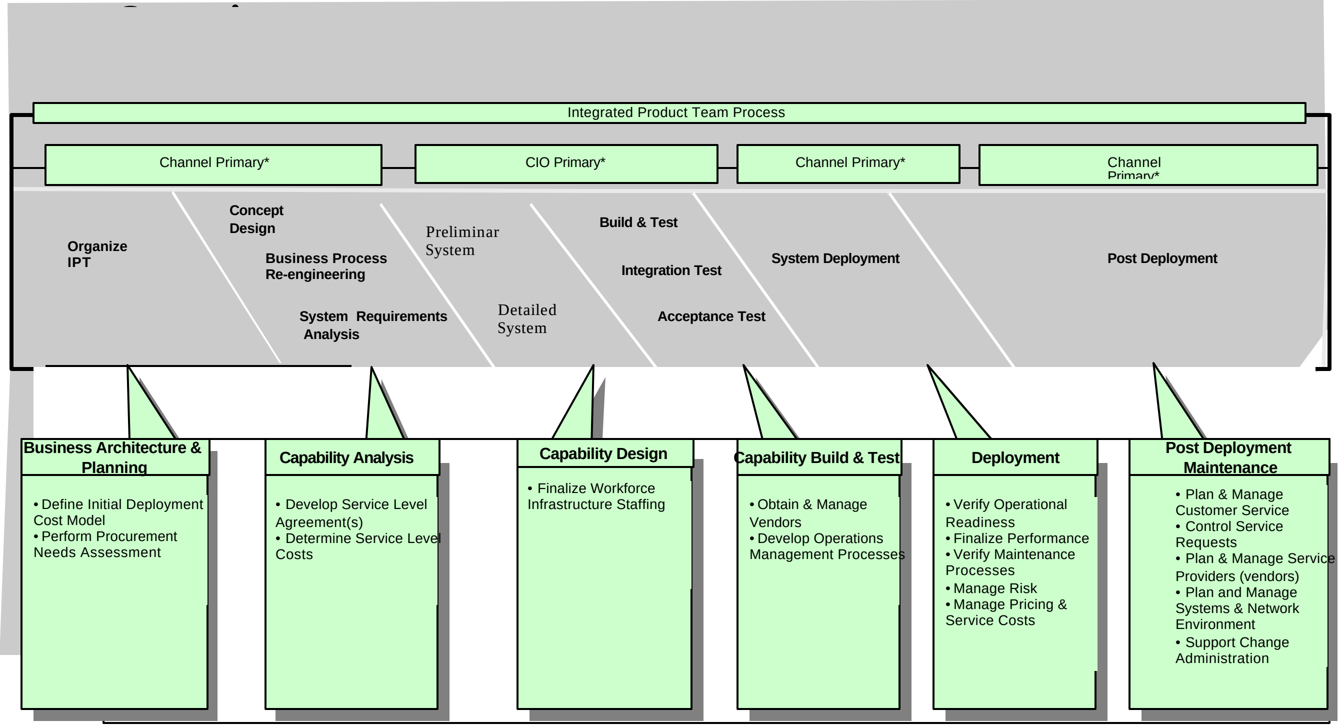
SFA does not have an enterprise level post deployment process. Nor does it have an integrated (software, hardware, infrastructure) approach throughout the software development life cycle. Most SFA systems are configured and managed by third party contractor organizations. These organizations are tasked with the upkeep and maintenance of the systems. To respond to the SFA external community needs/user inquiries/functional issues, SFA has multiple customer support centers. These customer service centers/call centers are operated by their legacy contractors. In the case when a problem has not been resolved, the SFA Ombudsman system is called in to support/resolve the issue.

Also, there is no central body, information technology help desk, in place to field technology problems. It should also be noted, there appears to be no coordinated investigation or response to problems and/or incidents which have cross channel concerns. This could mean problems discovered in one system (which may be similar), are rediscovered and fixed again. This strongly suggests a need for coordination at this level and for a set of repeatable processes.

1.3 IPT Post Deployment Process Overview

Presented here is a pictorial representation of the post deployment process and how it fits into SFA's integrated product team (IPT) process. At a glance, the activities intended for each phase of the deployment approach can be mapped to targeted goals within the IPT process. This diagram and those that follow, indicate the types of tasks required, the responsible lead organization and the participating/supporting groups. The next six diagrams break out each of the functional areas and indicates the parties required to execute them. Note, when it states the Channel as a lead or participant of an activity, it is suggested all Channels are represented. However, this will be left to the discretion of the task leader to determine how much involvement is needed.

Post Deployment Maintenance: High Level Process


Integrated Product Team Process
Channel Primary*
CIO Primary*
Channel Primary*
Channel Primary*
Organize IPT
Concept Design
Business Process Re-engineering
System Requirements Analysis
Preliminar System
Detailed System
Build & Test
Integration Test
Acceptance Test
System Deployment
Post Deployment
Business Architecture & Planning
• Define Initial Deployment Cost Model
• Perform Procurement Needs Assessment
Capability Analysis
• Develop Service Level Agreement(s)
• Determine Service Level Costs
Capability Design
• Finalize Workforce Infrastructure Staffing
Capability Build & Test
• Obtain & Manage Vendors
• Develop Operations Management Processes
Deployment
• Verify Operational Readiness
• Finalize Performance
• Verify Maintenance Processes
• Manage Risk
• Manage Pricing & Service Costs
Post Deployment Maintenance
• Plan & Manage Customer Service
• Control Service Requests
• Plan & Manage Service Providers (vendors)
• Plan and Manage Systems & Network Environment
• Support Change Administration

Business Architecture & Planning

Task	Channel	CIO	Legacy Contractors	Other
Develop Service Level Agreement(s)	P	L	P	CFO
Determine Service Level Costs	P	L		

(L = Leads Task, P = Participates in Task)

Capability Analysis

Task	Channel	CIO	Legacy Contractors	Other
Develop Service Level Agreement(s)	P	L	P	CFO
Determine Service Level Costs	P	L		

(L = Leads Task, P = Participates in Task)

Capability Design

Task	Channel	CIO	Legacy Contractors	Other
Finalize Workforce Infrastructure Staffing	L	P	P	CFO

(L = Leads Task, P = Participates in Task)

Capability Build & Test

Task	Channel	CIO	Legacy Contractors	Other
Obtain and Manage Vendors	P	L	P	
Develop Operation Management Processes	L	P		

(L = Leads Task, P = Participates in Task)

Deployment

Task	Channel	CIO	Legacy Contractors	Other
Verify Operational Readiness	L	P		
Finalize Performance		L	P	
Verify Maintenance Processes	L	P	P	
Manage Risk	L	P	P	
Manage Pricing & Service Costs	P	L		

(L = Leads Task, P = Participates in Task)

Post Deployment Maintenance

Task	Channel	CIO	Legacy Contractors	Other
Plan & Manage Customer Service	L	P		CFO
Control Service Requests	L	P	P	
Plan & Manage Service Providers (legacy contractors)	L	P	P	VDC
Plan and Manage Systems & Network Environment	L	P	P	VDC
Support Change Administration	L	P		CFO

(L = Leads Task, P = Participates in Task)

1.4 Document Organization

The post deployment approach includes the primary responsibilities of post deployment support in the system development life cycle process. Additionally, the steps required to fulfill these responsibilities, plus a high level design of the process and the organization structure that supports the post deployment are included.

- Section 1: Describes the overall purpose and scope of the post deployment approach. In addition, a high-level process summary of the functions included with the responsible organizational leads and participants, is included.

- Section 2: Describes the post deployment key concepts and processes. This section also describes the organization and the responsibilities allocated to each element of the organization for post deployment. The functions post deployment tools need to fulfill is covered in this sections, as is the relationship of post deployment with other processes and organizations.

- Section 3: Describes the next steps required to implement an enterprise-wide post deployment process.

1.5 Document Development Process

The following organizations and individuals were a source of information in writing this approach:

- SFA Enterprise IT Management: Wayne Wright, Denise Hill
- SFA Enterprise IT Services: David Moore, David Elliott, Phillip Wynn
- SFA E-Commerce Application Development: Constance Davis
- SFA CIO Business Manager: Harry Feely
- SFA CIO (COTR): Carol Seifert

The approach presented in this document derives its framework and functions from a series of Andersen Consulting's best practices in the area of operations management. The documents below supplied up to date reference material:

- Andersen Consulting Operations Management Best Practices
- Andersen Consulting Business Integration Methodology
- Andersen Consulting IT Framework (Service Management)
- Andersen Consulting MODE (Management Of Distributed Environments) Model

2 Post Deployment Maintenance Details

An enterprise post deployment program requires a number of important steps be taken to realize its benefits. This section of the approach summarizes those steps. The backbone for any good approach is a set of key concepts. These concepts are described briefly in the section to follow. The second step involves discussing the post deployment technical processes. Thirdly, there needs to be some discussion on the organization requirements necessary for the success of the enterprise. And finally understanding the concepts, technical processes and required organization structure, tools to do the job are the only things missing from the equation. The last section will provide a discussion on what types/tools are required to operate the enterprise post deployment operations. However, no tool recommendations will be made.

The post deployment maintenance phase focuses on achieving and sustaining the benefits of the new business capability implemented during the deployment phase. Post deployment maintenance is a lasting phase. Meaning, as time passes, continuous improvement techniques are used to ensure the success of the capability. These inputs to the post deployment maintenance phase are the key outcome of the delivering phases (capability build/test and capability deployment).
They include:

- An enabled business capability (with supporting infrastructure)
- A service level baseline, which formally describes the scope of services to be provided by the service provider (vendor/contractor) to the service customer (SFA business owners).

2.1 Key Concepts

The key concepts of post deployment are the technical principles that a post deployment program is based on. This section describes those concepts key to the success of a post deployment program at SFA.

The concepts that differentiate the SFA post deployment are:

- The focus for all activities is long-term (measured in years, not weeks or months).
- Post deployment maintenance does not consist of a series of projects that have a finite life span; activities are started once the business capability is deployed, and are ongoing simultaneously.
- Continuous improvement is used to sustain value. Continuous improvement means that periodically, the bar is raised to improve results. This process can achieve a reduction in cost and an increase in value.
- The post deployment maintenance phase focuses on outcomes. The deliverables for this phase are used to support the work in the phase itself, and are not delivered to the sponsoring organization. *T*he success of the post deployment maintenance phase depends on consistent and improved outcomes.

Key deliverables and outcomes from this phase include the operation of the business capability to achieve and sustain business value to the sponsoring organization. This is demonstrated by monthly performance reports and yearly assessment reports. Examples of these outcomes are provided below Note, each of the following equates to a task that is incorporated in the detailed project plan for implementing this post deployment approach.

- **Provide Service** task represents work performed in the delivering phases, including the people, processes, and technology related to the business capability. All of the other task packages are used to manage service provision.
- **Manage Human Assets** task manages the people.
- **Manage Service to Customer** task manages the process.
- **Manage Technology and Work Environment** task manages the technology.
- **Plan and Manage Service Provision** task provides the overall management layer that manages the results.
- **Improve Service and Productivity** task continues the operation of the right thing, not of a thing done right.
- The **Manage Service from Domains and Provide Service** task packages provide an orderly and controlled way in which services are requested by the service customer, and provided by the operational domains.

The scope or size of the post deployment maintenance phase depends mainly on business volumes. Additional factors that affect scope include the number of personnel, skill sets available, number of transactions, business maturity, and the sponsoring organization's ability to manage and implement change.

This leads to a discussion on success factors. Listed below are some key ones to keep in mind during the post deployment maintenance phase.

Success Factors

- **Focus on the customers of the service**---A formal service level agreement (SLA) should be signed by the service provider and the customer of the service. This agreement should detail the processes, people, and interfaces affected by the service.

- **Manage the service as a process**---Use process metrics and performance goals for the business process as well as for the application and people involved. The goals and metrics should support the business case and value proposition.

- **Focus on quality and continuous improvement**---Instill the capacity to change in the culture of the service provider. Also, measure the success of the service against established performance goals, and use the measure to adjust the process as required. Note, this activity should be aligned with the SFA performance management program.

- **Align the level of resources with the service levels and business volumes**---Be aware of fluctuations in service levels and volumes to keep the level of people, equipment, and facilities in tune with service demands. This phase revolves around continuous improvement. Therefore, flexibility should be built in to allow adjustments to service level, volume levels and operational levels.

- **Instill a performance focus in people**---A performance based organizational approach is being utilized. Communicate the delivery goals very clearly. We should be explain there is a tie between compensation to performance, and provide an environment that is conducive to quality work. As part of the communications plan, SFA team members, as well as contractors, should be told what is expected from them. Further it should explained evaluations, rewards, and/or critiqued performance will be done against these communicated expectations.

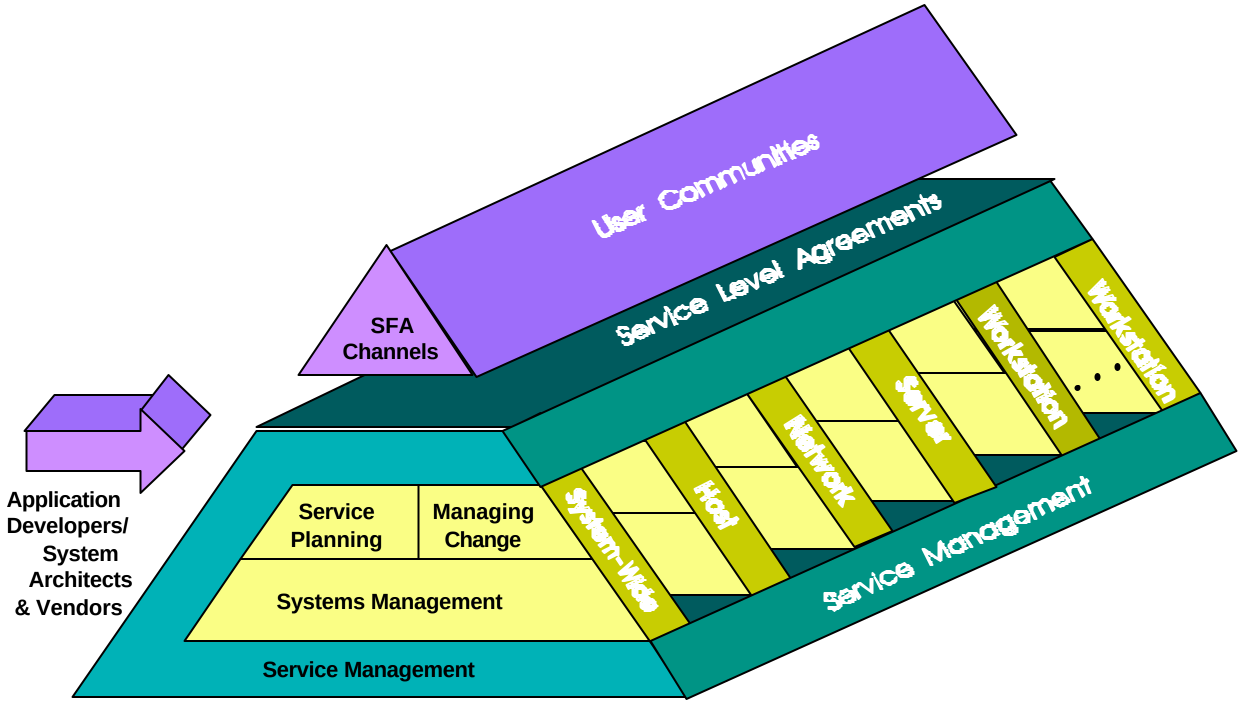
2.2 Post Deployment Design

To introduce the post deployment approach, this section has been broken into three parts. First, the approach diagram was previously presented in section 1.4 of this document. It indicated the touch points within the products & services release life cycle the maintenance support activities occurred and their relative timeframes. This follows the process previously outlined in the deployment approach document (business architecture and planning, capability analysis, capability design, capability build and test, and deployment). Second, a discussion of the operational model or framework the approach is based on is given. And thirdly, for each process of the proposed SFA operational model, there are a series of sub-processes that outline the maintenance activity. Their definitions and importance to SFA are outlined in this section.

2.2.1 Post Deployment Operational Model

The approach can be logically represented by the picture below. Notice, it has been broken down into the following processes:

- Service Management
- Systems Management
- Service Planning
- Managing Change



Service Management

Service management is the direct interface to the users of the SFA distributed systems. In SFA, this relates to the legacy contractors and vendors performing a task(s) on a routine basis to sustain the SFA systems. SFA users are depicted at the top of the diagram to represent the fact that a distributed system is managed in order to support the users of the system. Ultimately, the users of the system will define the service offered to the customer/client base. Users interface with service management exclusively, as they should only see the services being provided to them. Users should not need to see how the services are provided. An example of service management would be the Ombudsman system. The help desk service it provides is available to all SFA Channel personnel.

Service management is also the direct interface to the application developers, system architects and vendors for the SFA systems. Each of these groups has requirements for, and introduces change into, the distributed environment.

Systems Management

Systems management involves all functions required for the day today operation of the distributed system (e.g. event monitoring, failure control, performance monitoring, etc.). In SFA this relates to the activities of the legacy contractors managing the SFA Channel owned systems. For example, the legacy contractors/vendors manage the systems of the Ombudsman system. Systems management activities must take place in an ongoing manner, regardless of the changes taking place within the distributed environment.

Service Planning
Service planning encompasses all of the functions which outline SFA's tactical and strategic planning that needs to take place in order to manage a distributed environment effectively. It should be noted, the greatest period of change in the management of SFA's systems will be during the initial phase of a business capability rollout (and installation). An example of this would be planning for the rollout of the SFA new intranet web site in the SFA Director of Communications systems implementation plans.

Managing Change
Managing change includes all of the functions that are either new or significantly different in a distributed environment (e.g. software & data distribution, license management, etc.). However, in some cases, not only have the management procedures of the system changed, but the system itself has changed. This significantly increases the amount of focus required to ensure the environment is being managed appropriately.

2.2.2 Post Deployment Processes

2.2.2.1 Service Management

The service management process consists of a set of principles by which SFA can manage the operation of a business capability by measuring the capability's actual contribution to business value. An example of SFA service management is the FMS (financial management system) which provides accounting for management and for various SFA line organizations. The customers of FMS are all internal. They are users of the information and are also judges of how valuable FMS' services are to the business.

Definition of a service interface

The service management framework requires the definition of a service interface: a point at which channel users of a business capability can trigger processes and receive the outcomes of those processes. The service interface is the point where the performance of the process (its timeliness, quality, cost, etc.) can be measured, and therefore managed. The service interface is defined as the boundary between two organizations: the service provider (which owns and operates the process) and the service customer (which owns the outcome). Following the scenario above, an example of a service interface could be a report generated by the FMS for one of the SFA Channel managers. The speed of computing and accuracy of the report could be a service interface between the FMS and SFA Channel.

Definition of a service level agreement

The service provider and the SFA Channel customer negotiate a service baseline that specifies the scope of services to be provided. This service level agreement specifies, for each service item, the expected performance level for that service item. It also describes the mechanism for negotiating the provision of services that are not included in the baseline, such as exceptional requests or new requirements. Note, the detailed functions involved in this process are discussed below in this section.

Application of a customer-focused service management

This is the direction the Modernization Partner is attempting to move the SFA towards. In a customer-focused, process-oriented implementation, a business capability is aligned to an end-to-end business process that provides a service to an external or internal SFA customer. The service level agreement would be based on the process design and aligned with the organizational structure. The metrics used to evaluate service performance would be the performance indicators of the business capability. The SFA channels play a significant role in establishing these performance indicators.

To illustrate this concept, consider the following example of business capabilities. The first is an SFA call center (Ombudsman). The call center has two main types of customers: SFA internal and external. The external customers are those who phone the call center when they are in need of service (students, schools, financial organizations. The internal customer is the company's own management, especially those who are in charge of keeping customers satisfied. These are the people who will judge whether the call center provides the expected business value.

However, there are several challenges ahead. Such as, the delivered business capability may not be as well aligned with organizational boundaries. Those who operate the capability may be under the direct hierarchical control of those who use it, meaning it may not be possible to negotiate any significant service level baseline. The business processes are often not owned by those who execute them. The people who operate the capability may be held responsible for reaching specified performance goals, but typically have little authority to change the processes if the goals are not reached. In this case, it is difficult for an SFA channel to achieve the business performance targeted for a new business capability. Also, even if the initial goal is reached, it may be difficult to sustain and improve the performance over time.

In situations like the ones previously described, it would still be possible to apply the service management process to parts of the business capability. In the case of the accounting department, the accountants may not believe that the rest of the company is their customer. Almost always, however, the accountants are themselves users of the services of some other organization. Thus, the service management process can be used for a well-defined subset of the business capability.

Service Level Agreement (SLA) Details

Conceptually, SLAs are not new and have been used for a variety of ways, including: the outsourcing of an entire business function to a third party, the provision of internal IT support services for a particular business application, or the outsourcing of the help desk and user support services.

Client/server and distributed computing environments increase the importance of using SLAs and operating level agreements (OLA) to gauge the business effectiveness of the systems. In the client/server or distributed processing environment many designs and configuration alternatives are available that impact a given system's response time, availability, development cost, and ongoing operational costs. An SLA clarifies the business objectives and constraints for an application system, and forms the basis for both application design and system configuration choices.

It is not uncommon to find requirements in a service level agreement that can only be supported by being designed into the application or enterprise technical architecture. For example, the response time reporting requirements for a client/server application may not be able to be fulfilled by primitive application monitoring capabilities of operating environments such as Windows NT. In this case, it may be necessary to design into the application the ability to collect and report statistics on end user response times or productivity.

In addition to providing guidance to application and systems design, SLAs help manage user expectations of the IT support services. Similarly, OLAs will help manage IT expectations of vendors, and the various support groups within SFA.

SLA Definition

An SLA is an agreement between the **SFA Channel customers** of the service and those responsible for **managing the service**. It defines the level of service which will be delivered to the users by those managing the service. It defines:

- who the customers are and the service levels they require
- roles and responsibilities for suppliers and customers
- rewards for meeting or exceeding service levels
- monitoring procedures
- costs
- contractual arrangements
- review mechanism
- formal interfaces between users and information technology (IT) services

SLA Control

SLA control assures that agreed upon service levels are consistently being met by regularly assessing services delivered against the target service levels defined in the SLAs. If an SLA is being violated, SLA Control will take the appropriate action to determine what is causing the violation and initiate a fix to ensure expected service delivery. SLA control also ensures SLAs are being met in the most efficient and productive manner possible.

SLA Reporting

SLA reporting provides regular information on how well the service levels are being achieved. This mechanism provides those managing SLAs and service customers with historical reports tracking the service delivered over a particular period of time.

SLA Review

SLA review formally discusses SLA reports with service customers. SLA review provides customers with a formal opportunity to discuss their service arrangements, potential changes to their agreements and methods for improving the quality of services delivered to them.

OLA Definition

An OLA is an agreement between those responsible for **managing the service** (system), and those **delivering service** (service providers) to the users of the service (system). An OLA outlines the type of service to be delivered, by the service providers to their users. OLA definition works with service providers to define:

- whether a particular service level can be met, and how it will be met through operational levels
- which provider(s) can provide a service, or part of a service
- roles and responsibilities
- what constitutes a failure to meet the OLA, and corresponding penalties (if appropriate)
- monitoring procedures
- cost structures
- how the service will be measured
- contractual arrangements with the providers.

Formal OLAs will be defined for suppliers external to the IS organization, although it is quite possible that further informal OLAs will be created for internal suppliers.

OLA Control

OLA control assures that agreed upon service levels are consistently being met by regularly and frequently assessing service delivered against the target service levels defined in the OLAs. If an OLA is being violated, OLA control will take the appropriate action to determine where the violation is occurring, how the violation will be fixed and when proper service will be restored.

OLA Reporting

OLA reporting provides regular information on how well the service levels are being provided by a service provider or across a particular domain. This mechanism provides those managing OLAs and service providers with reports tracking the service delivered over a particular period of time.

OLA Review

OLA review formally discusses OLA reports with service providers. OLA Review offers service providers a formal opportunity to discuss their service arrangements, potential changes to their agreements and methods for improving the quality of service delivered to them.

Help Desk Functions

When compared with the more traditional centralized environment, there will be more support groups in the IT department to provide the range of skills needed for the distributed environment. There is more opportunity for incidents, requests and problems to get 'lost' between teams, and for issues to be passed from team to team without resolution. Therefore, the procedures to manage the progression of incidents, requests and problems to closure, and the management reporting associated with them, need to be more rigorous than is normally required for centralized systems.

Incident Management

An incident is a single occurrence of an issue which affects the delivery or normal or expected service. Incident Management provides the interface between the users of the service and those operating and supporting the service when an incident arises. Incident Management is responsible for:

- receiving incidents from users
- informing users of known workarounds where possible
- ensuring that support personnel are working on an incident
- keeping users informed of incident resolution progress
- ensuring incidents do not get lost as they are passed around support teams
- informing users when incidents have been resolved and ensuring resolution is complete
- ensuring that outstanding incidents are resolved in a timely manner.

Incident management should strive to resolve as high a proportion of incidents as possible prior to passing them on to other areas. Incident management will use its business and product knowledge together with known problem checklists and other diagnostic aids to deliver high quality support services.

Problem Management

A problem is the underlying cause of one or more incidents. Problem management utilizes the skills of experts and support groups to fix and prevent recurring incidents by determining and fixing the underlying problems causing those incidents. Within problem management, related incidents are correlated to problems and ultimately to change or order requests. All problems are logged, tracked and archived. Where possible, workarounds are determined and information regarding the workarounds is distributed to the appropriate support personnel and user communities.

Request Management

Request management is responsible for coordinating and controlling all activities necessary to fulfill a request from a user, vendor or developer. Request management determines if and when requests will be fulfilled through interaction with the particular function(s) impacted by the request. Following such interaction, accepted requests can either be:

- raised as change requests with configuration management, and
- planned, executed and tracked by Help Desk.

2.2.2.2 Systems Management

Systems management involves all functions required for the day to day operations of the whole system (hardware, software and infrastructure). Regardless of the changes taking place in the system, systems management activities must take place in an on-going manner. Systems management includes the following categories of activities:

- Production control,
- monitoring
- failure control,
- security management and
- systems management planning.

Production Control

- Production control manages the day to day operation of the systems and ensures that production activities are performed and controlled as required. This includes:
- Production scheduling: Scheduling and execution of jobs.
- Print management: Managing and monitoring all printing done across the distributed system.
- File transfer and control: Initiating and monitoring file transfers throughout the system as part of business processing (e.g. nightly updates).
- System startup and shutdown: Activities necessary for the startup and shutdown of the entire system (hardware and software) or portions of the system.
- Mass storage management: Activities related to the handling of various types of centralized and distributed storage media, including monitoring and controlling of storage resources and their usage.
- Backup and restore management: All backup and restore activities for system software, applications and data.
- Archiving: Moving files and data sets from one device to another. This also includes cleaning systems by removing files that are no longer used.

Monitoring

- Monitoring verifies that the system is continually functioning in accordance with defined service levels. This includes:
- Event management: Collecting and analyzing system events to monitor the status of the system components.
- Performance management: Diagnosis of the system performance and initiating corrective and pre-emptive actions to ensure sufficient resources are available at all times.
- Physical site management: Control and support of all devices in the physical areas (computer rooms, etc.) to ensure the environment is controlled properly.

Failure Control

- Failure control covers the detection and correction of faults within the system. It ensures that service delivery is restored after the system fails. In addition it controls maintenance of all hardware components within the system. It includes the following activities:
- Fault management: Diagnosis, isolation and correction of faults in the system.
- Recovery: Activities needed to restore service delivery after a system failure.

- Disaster recovery: Activities needed, in the event of a significant system failure, to re-route system resources to a secondary, stable configuration.
- Hardware maintenance: implementing hardware maintenance plans, monitoring them for effectiveness and recording activities for each hardware device.

Security Management

- Security management covers all activities and measures to reduce the risks of unauthorized access from outside and unauthorized actions by users from the inside. A system will never be fully secure and therefore security solutions are aimed at reducing the risk to an acceptable level. Security management includes:
- System level security management: Reducing the risk from unauthorized access to the system or to system components (e.g. system and network logon, etc.)
- Maintenance of user (authorization) profiles: Maintaining user profiles to ensure users can and can only access those components they are authorized to use.

Systems Management Planning

- Systems management planning must be performed to provide consistent day to day operation and service levels. The key areas in systems management planning are:
- Physical site planning: Planning of what is necessary at a physical site (e.g. computer room, work place) to comply with any SLA or health/safety/regulatory requirements in existence.
- Security planning: Planning of the security of all components in the system (e.g. computers, communication lines, physical facilities, personnel, documentation, etc.) and determination/co-ordination of the security requirements.
- Capacity modeling and planning: System modeling and planning to ensure that adequate resources will be in place to meet the SLA requirements, keeping in mind other operational requirements which may require additional capacity. Resources include physical facilities, computers, memory/disk space, communication lines and personnel.
- Contingency planning: Planning, testing and monitoring the ability to switch to alternate resources when a portion of the system is or cannot remain functional.
- Recovery planning: Determination of recovery strategies and plans to restore services that have been interrupted.
- Disaster recovery planning: Determination of the requirements and strategy for disaster recovery services, based on agreed upon SLAs.
- Hardware maintenance planning: Determination of overall maintenance plans for hardware.

2.2.2.3 Service Planning

Service management planning at SFA would include service costing and pricing which projects and monitors costs for the management of operations, provision of service, and equipment installation. Service planning also includes training planning.

Service Costing and Pricing

Service Costing and Pricing projects and monitors costs for the management of operations, provision of service, equipment installation, etc. Based upon the projected costs and business needs, a service pricing strategy may be developed to re-allocate costs within the organization. If developed, the service pricing strategy will be documented, communicated to the users, monitored and adjusted to ensure that it is both comprehensive and fair.

Service costing and pricing function will ensure that the real cost of service provision is recovered/charged back to the business.

Training Planning

Training Planning identifies the needs of those who will require training within the distributed environment based on the agreed upon SLAs. Training may be required for: users of the system, customer service personnel (e.g. help desk), and support or operations personnel.

Systems Management Planning

Systems Management Planning brings together the various elements required to manage a system. These elements include: physical site planning, security planning, capacity modeling and planning to ensure that adequate resources will be in place to meet the SLA requirements, contingency planning, recovery planning, disaster recovery planning, and hardware maintenance planning.

Physical Site Planning

Physical Site Planning considers what is necessary at a physical site to comply with any SLA, health and safety, or regulatory requirements in existence and prepares a plan to meet those requirements.

Security Planning

Security Planning addresses all of the components of a system (e.g. computers, communication lines, physical facilities, personnel, documentation, etc.) and determines/co-ordinates the security requirements (e.g. from SLAs, business and regulatory requirements). Based on the requirements, Security Planning devices a security plan/strategy.

Capacity Planning and Review

Capacity Planning and Review ensures that adequate resources will be in place to meet SLA requirements, keeping in mind operational requirements which may require additional capacity. Resources can include such things as: physical facilities, computers, memory/disk space, communications lines and personnel. Through this function, changes to the existing environment will be determined, modeled and planned according to the necessary requirements.

System capacity monitoring and planning will be conducted to ensure that the capability to meet SLAs is in place. As the requirements of the systems at SFA increase it is important to ensure that expansion of the supporting infrastructure is planned for and implemented commensurately.

Contingency Planning

Contingency planning determines the requirements for, plans, tests and monitors the ability to switch to alternate resources within the distributed system when a portion of the system is not or cannot remain functional. Contingency planning must ensure that its plans meet the agreed upon SLAs.

Contingency Planning is not considered to be separate operational function at SFA. The contingency planning functionality is covered by the capacity planing and the disaster recovery planning functions.
As a rule, systems installed at SFA will have redundancy built-in.
Intention is to keep a minimum level of spare (standard) components at SFA to ensure that systems can be recovered within the agreed SLAs.

Recovery Planning
Recovery Planning determines recovery strategies and plans to restore service after it has been interrupted. Recovery/recovery planning is not considered to be a separate operational function at SFA. Recovery planning functionality is addressed through the disaster recovery planning.

Disaster Recovery Planning
Disaster recovery planning determines what the requirements are for disaster recovery services based on agreed upon SLAs. This planning process develops the strategy for recovering systems, or portions of systems, in the event of a significant system failure. The contingency plans must consider failure of both centralized and remote components and strategies for the recovery of these systems.

Hardware Maintenance Planning
Hardware maintenance planning protects a SFA's investment in it's distributed environment's resources by determining overall maintenance plans based upon agreed SLAs.

2.2.2.4 Managing Change

Managing change includes all of the functions required to control introduction of change in a complex environment (e.g. software and data distribution, license management). The impact of change in an organization is substantial, so this key process requires extensive coordination and defined communication points in order for an IT organization to successfully manage its workload.

Controlling
Controlling includes change control, asset management, rollout management, release control, migration control, and license management.

Change Control
Change control is responsible for co-ordination and controlling all change administration activities within the distributed environment. Change control determines if and when a change will be carried out through discussion with any function that will be impacted by the change. Following such discussion, accepted changes will be planned at a high-level and tracked through to completion.

These policies/procedures will be flexible enough to accommodate the frequent and rapid changes required but they will also be rigid enough to ensure that operational control and accountability is retained.

The change management process will ensure that all new systems, system updates and system changes being introduced to the production environment are fully tested and have appropriate back-out capability. The change management procedure will also effect daily operations, ensuring that accountability is maintained by requiring all changes (including system re-starts) to be recorded. All changes, except for changes resulting from an urgent fix, (hardware and software, scheduled and un-scheduled) will require a change management system record to be generated. The detail changes resulting from urgent fixes will be documented via some configuration management system tool.

Asset Management

Asset management ensures that all assets are registered within the inventory system and that detailed information for registered assets is updated and validated throughout the asset's lifetime. This information will be required for such activities as managing service levels, managing change, assisting in incident and problem resolution and providing necessary financial information to the organization.

Asset management will serve dual purpose - track financial data/asset value for the financial assessment purposes (e.g. company value, depreciation), and will be used to track all assets to assists with the obsolescence planning and the equipment redistribution/redeployment and prevent fraud, waste, and abuse.

Rollout Management

Rollout management is concerned with delivering new sites or services to existing sites on-time based on the rollout schedule. Rollout management monitors the rollout progress of all functions against the rollout schedule takes place regularly to determine how well rollout is progressing and to make any adjustments to the rollout schedule based upon any problems or issues which arise.

Release Control

Release control is concerned with delivering a release on-time based upon the release schedule. It monitors the release progress of all activities against the schedule to ensure that the schedule is maintained. Review of the release schedule takes place regularly to determine how well the release is progressing and to make any adjustments to the release schedule based upon any issues or problems which arise.

Migration Control

Migration control co-ordinates the movement of a release package from the development environment to the test environment, and ultimately from the test environment to the production environment. It's responsibilities are to manage access to the release package and to maintain the integrity of a release package.

License Management

License management ensures that software licenses are being maintained throughout the distributed system and that license agreements are not being violated. License management will be linked to the asset register. Assets within the asset register that require licenses (operating systems, software) will be exported to a license register.

Product Validation

Product validation tests potential hardware and software for the distributed environment prior to procurement to determine how well a product will fulfil the requirements identified. It also ensures that the implementation of a new product will not adversely affect the existing environment.

To ensure that the product will satisfy SFA's minimal requirements (functional, security, architectural, etc.) technical standards and guidelines must be followed for both "of-the-shelf" products and the in-house developed solutions. These standards will be provided by the enterprise architecture team.

Release Testing

Release testing receives the proper version of a release package (e.g. software, data, procedures, support materials) and tests the release of the upgrade in a test environment to ensure that the:

- entire release package is compatible with the existing environment
- release package may be released successfully by the planned methods
- release can be supported by support personnel

Implementing

Implementing addresses: procurement which is responsible for ensuring that the necessary quantities of equipment are purchased and delivered on-time to the appropriate locations, initial installation, component configuration which provides a mechanism to configure equipment which has configuration parameters, software and data distribution, and user administration.

Procurement

Procurement is responsible for ensuring that the necessary quantities of equipment (both hardware and software) are purchased and delivered on-time to the appropriate locations. Procurement is also responsible for logging into the inventory as they are received.

Initial Installation

Initial installation prepares the physical location for the rollout of a new site or service, pre-assembles the equipment (hardware and software) based on developed specifications, installs the equipment and tests that the equipment is fully functional prior to allowing the users to utilize the system in a production environment.

A checklist will be developed that covers what tasks need to be performed and checked during different phases of the implementation of systems. The checklist will be used by the various IT groups as they implement their functions.

System Component Configuration

This provides a mechanism to configure equipment (e.g. hardware and software) which has configuration parameters to set and to manage the inter-relationships between configured components within the system. Configuration information for particular equipment must be coordinated across the system to ensure that all equipment can function together properly.

System component configuration is tied closely to initial installation and is usually performed by the same team at the time of initial installation. Each support area (virtual data center, Infrastructure Development, Database Services, etc) can provide assistance with the relevant system components configuration.

Software and Data Distribution

Software and data distribution sends out the correct version of the release package to the distribution locations and updates the locations with the contents of the release package e.g. software, data, configuration information, procedures and training/support materials.

As the number of systems and the volume of change increases an automated electronic method of software distribution may be required . A system may be needed to distribute data and software across many systems, whilst minimizing the risk from potential problems.

User Administration

User administration handles the day-to-day tasks involved in administering users on the system. These tasks include such things as: adding new users, changing user IDs, re-establishing user passwords, maintaining groups of users, etc.

Organizations and Responsibilities

The post deployment approach aligns with the processes defined in the deployment and configuration management approaches. Involvement in post deployment activities by the proper organizations will ensure effective lines of authority, supervision, and communication. This section describes the post deployment related project organizations, details the authority and the specific responsibilities for post deployment for each element throughout the project life cycle.

2.2.3 OCIO, OCFO, GMs, and Modernization Partner

Representatives of the Office of the Chief Information Officer, Office of the Chief Financial Officer, General Managers (students, schools, financial partners) and the Modernization Partner approve the post deployment maintenance planning, support policies, service & operating level agreements and associated high level procedures to maintain and support SFA's deployed business capabilities. SFA strategic planning for post deployment requires representation from this group to effective cover all areas of concern. Note, the low level detailed policies and procedures will be tasked to departments or groups within these organizations mentioned above.

2.2.4 Post Deployment Team

The post deployment or maintenance team should consist of trained application analysts, database administrators, network administrators, SFA Channel subject matter experts (not full-time), and system administrators. They should be augmented on an as needed basis by SFA representatives of system integration & testing, configuration management, application development team, and the deployment teams. A post deployment coordinator (lead) should be assigned to each integrated product team (IPT). These individuals are the points of contact for all issues regarding post deployment for the specified project prior to actual deployment. Once deployed, the post deployment maintenance team will assume responsibility.

2.2.5 Configuration Management Organization

The CM will be responsible for maintaining the released baseline. This function maintains the system databases that document change status, prepare and distribute configuration status accounting and tracking reports to appropriate project and client personnel. The CM will provide guidance and assistance on all SFA CM issues. The CM responsibilities will include the following major activities:

- Controlling product baseline and all integration and testing configurations.
- Ensuring the change and report tracking is kept current for change request and maintaining a history of such changes.
- Moving source code into a CM controlled area and performing system builds. Maintaining the system baselines.
- Packaging the source code (and database structures) for post deployment.

- Preparing project master release tapes from the CM library and delivering them to the post deployment lead for distribution to the client environment(s).
- Capturing and maintaining post deployment log of system discrepancies, issues, problem reports on the delivered configuration items.

2.2.6 eCommerce Application Development Team(s)

The development team lead and the respective project post deployment coordinator are responsible for identifying and packaging each of the configuration items which make up a unique version and handing this off to the post deployment team. Actually, the physical handling of the configuration items will be conducted by the configuration management team. The development team lead, with the help of the post deployment coordinator, must ensure that the integrity of the solution is maintained once a change has been implemented in the release baseline.

2.2.7 Virtual Data Center (VDC)

The virtual data center team will be responsible for controlling and validating all hardware baselines. This includes the configuration, maintenance, upgrade and tracking of all infrastructure (hardware, system software, communications, database, network) components.

Configuration item change(s)/update(s) will be coordinated with the post deployment team. In addition, the virtual data center will support performance and capacity monitoring tasks.

2.3 Post Deployment Support Summary

The following matrices link the organizational units to the service management, system management, service planning and managing change functions:

	Enterprise IT Management	SFA Operations Support	Enterprise IT eCommerce Applications	Channel Applications Support	Enterprise IT Services	Channel Project Technical	Channel Management Support
Service Management							
SLA Management							
SLA Definition						X	X
SLA Reporting						X	X
SLA Control						X	X
SLA Review						X	X
OLA Management							
OLA Definition						X	X
OLA Reporting						X	X
OLA Control						X	X
OLA Review						X	X
Help Desk							
Incident Mgmt		X		X		X	X
Problem Mgmt		X	X	X	X	X	X
Request Mgmt		X		X		X	X
Quality Management							
Quality Mgmt		X			X	X	X
Training					X	X	X
Administration							
Billing & Accounting			X			X	X
Contract Mgmt			X			X	X

X = Organizational Unit Performs Function

Systems Management

	Enterprise IT Management	SFA Operations Support	Enterprise IT eCommerce Applications	Channel Applications Support	Enterprise IT Services	Channel Project Technical	Channel Management Support
Production Control							
Production Scheduling		X			X	X	X
Print Management			X		X	X	X
File Transfer & Control		X	X		X	X	X
System Startup & Shutdown		X	X		X	X	X
Mass Storage Management		X	X		X	X	X
Backup / Restore Management		X	X		X	X	X
Archiving		X	X		X	X	X
Monitoring							
Event Management		X			X		
Performance Management		X			X		
Physical Site Management							
Failure Control							
Fault Management					X	X	X
Recovery					X	X	X
Disaster Recovery					X	X	X
Hardware Maintenance					X	X	X
Security Management							
Security Management					X	X	X

Service Planning

	Enterprise IT Management	SFA Operations Support	Enterprise IT eCommerce Applications	Channel Applications Support	Enterprise IT Services	Channel Project Technical	Channel Management Support
Service Management Planning							
Service Costing & Pricing	X				X	X	X
Training Planning				X		X	X
Systems Management Planning							
Physical Site Planning					X	X	X
Security Planning	X				X	X	X
Capacity Modeling & Planning					X	X	X
Contingency Planning					X	X	X
Recovery Planning					X	X	X
Disaster Recovery Planning					X	X	X
Hardware Maintenance Planning					X	X	X
Managing Change Planning							
Rollout Planning		X			X	X	X
Release Planning	X	X	X		X	X	X
Procurement Planning	X		X			X	X
Strategic Planning							
Strategic Planning	X		X				

Managing Change

	Enterprise IT Management	SFA Operations Support	Enterprise IT eCommerce Applications	Channel Applications Support	Enterprise IT Services	Channel Project Technical	Channel Management Support
Controlling							
Change Control		X	X		X		
Asset Managemen	X		X			X	X
Rollout Management		X			X	X	X
Release Control	X					X	X
Migration Control		X			X	X	X
License Management			X			X	X
Testing							
Product Validation	X		X			X	X
Release Testing	X	X	X		X	X	X
Implementing							
Procurement		X			X	X	X
Initial Installation		X			X	X	X
Component Config		X			X	X	X
S/W & Data Dist	X			X	X	X	X
User Administration					X	X	X

3 Next Steps and Implementation Plan

3.1 Next Steps

3.1.1 Identify the Implementers of Enterprise Post Deployment Maintenance

Upon the decision to move forward, the first step required to develop and/or augment an SFA post deployment presence is to build the support organization that is going to drive it. However, to start, someone or some team must be defined to lead the charge. They should be tasked with the responsibility for obtaining and identifying the resources and implementing the organizational structure for the SFA. Tasked with this responsibility, one of the first decisions that needs to be made is whether the SFA would be better suited if the post deployment team were composed of SFA staffers or whether it should be outsourced. Our recommendation is the Modernization Partner Enterprise architecture team – Delivery QA unit, be tasked to work with the CIO Enterprise IT Management organization to put implement the necessary structures, policies, procedures and guidelines. This is recommended because the potential time lag in identifying and mobilizing the appropriately skilled SFA personnel, could be offset by the readily available resources of Modernization Partner. Utilizing Modernization Partner personnel at least for the first phase of implementation would afford the SFA ample time to conduct a personnel search (and training). Upon, the conclusion of the first phase and once the organization has become operational, at the SFA discretion, the post deployment Team could revert to a SFA operation.

3.1.2 Define Scope of Implementation and Timeline

The second step is to define the scope of the implementation and determine how much time should be allocated to implement it. Since a number of elements that support post deployment are in currently in place at SFA, this implementation could begin immediately. The effort referred to here is more of a coordination and collaborative one that involves the information technology community at SFA. The scope in this case could mean multiple things.

A phased implementation approach should be used because its magnitude spans numerous groups at SFA. A detailed project plan should be developed outlining all the tasks/objectives with measurable milestones. One individual working with the CIO Enterprise IT Management, IT Services, IT eCommerce Applications teams and channel representatives could produce the detailed project plan in the implementation phase of this approach.

3.1.3 Identify Key Post Deployment Leadership

The third step is to mobilize the maintenance leadership team (obtain resource commitments, conduct training – if required, make task assignments and begin working the project plan tasks). This could be the kick-off meeting for the post deployment maintenance implementation. A primary goal of this step will be to level set all organizations involved. SFA organizations that should be in attendance are: the CIO Enterprise IT Management, IT Services, IT eCommerce Applications, CFO representatives and the business owners (GMs, Student, Schools, Financial Partners representatives). All roles should be addressed at this meeting. Secondly, key or critical vendor contractor relationships for maintenance activities need to be confirmed. Commitment levels and measurable milestones should be identified and contract negotiations (if necessary) should be firmed up during this period.

3.1.4 Establish Relationship with Integrated Product Teams (IPTs)

This requires the integration of a key post deployment resource into the IPT process. This integration could happen as early as the build / test phase of the development effort. The goal is to be aware of the capability’s needs once it has been deployed. Therefore, the tasking is a operational requirements gathering and resource mapping exercise. This work should be done in conjunction with the deployment team representative’s effort. Most importantly, the post deployment resource should be working with the business owner representatives to obtain service level and operating level agreements. This is by far the most critical activity that can begin. One goal of post deployment maintenance is tracking and monitoring the deployed system’s performance. These agreements serve as the yard stick all service provided will be judged.

3.2 Implementation Plan

3.2.1 Assemble Organization for Post Deployment Maintenance

A post deployment maintenance organization is required to support and sustain the systems capability that has been deployed. There are a number of organizations that take are required to support these business capabilities. The task here is to 1) document the detailed role descriptions required; 2) identify the key organizations (and resources if possible); 3) recruit candidates (augment with Modernization Partner personnel until SFA personnel become available and trained; 4) and train the key team members in the post deployment maintenance processes.

This team will initiate the post deployment activities by integrating the post deployment coordinators into the latter stages of the integrated product teams (IPTs). Within the IPTs the coordinators would have the broad brush view necessary for attending to all SFA concerns about the deployed capability. This extended IPT team would support the initial needs of the post deployment activities. After deployment has been completed, the maintenance team lead, would turn over all pertinent reports, statistics, open issues to the post deployment maintenance organization. They would then become responsible for providing post deployment support to the SFA system.

3.2.2 Train Personnel in Maintenance Processes and Tools

As a best practice suggestion, post deployment/maintenance support require very efficient and highly expert individuals in various technologies. This is a highly desirable trait for the SFA environment as well. To this end, training is a key factor to a smoothly operating technology support organization. Therefore, the following is suggested:

Train Personnel in Overall Process(es)

The first step is to ensure that everybody in the SFA organization affected by post deployment understands the overall process. An overview of the sub-processes should be conducted for key SFA representatives initially. This training should teach the basics. Every person involved in the post deployment process should attend this training

Technology Training

Upon the identification of the key resources within SFA, technical tools training should be conducted. This may not be required of SFA personnel if vendor contractor are tasked with this support. However, new tools recommended will be subject to the SFA tool criteria and evaluations developed by the Modernization Partner enterprise architecture team for the CIO Enterprise IT Management group. Any new tools will be subject to the common operating environment and development standard guidelines. Note, these guidelines have been published in a separate document.

4 Appendix

4.1 Information Flow Diagrams

4.1.1 SLA and OLA Management

The following diagram is a best practice that shows the interfaces between all the service level agreement (SLA) and operating level agreement (OLA) management functions. The hand-offs between the various functions are critical, and are detailed in the table following the diagram:

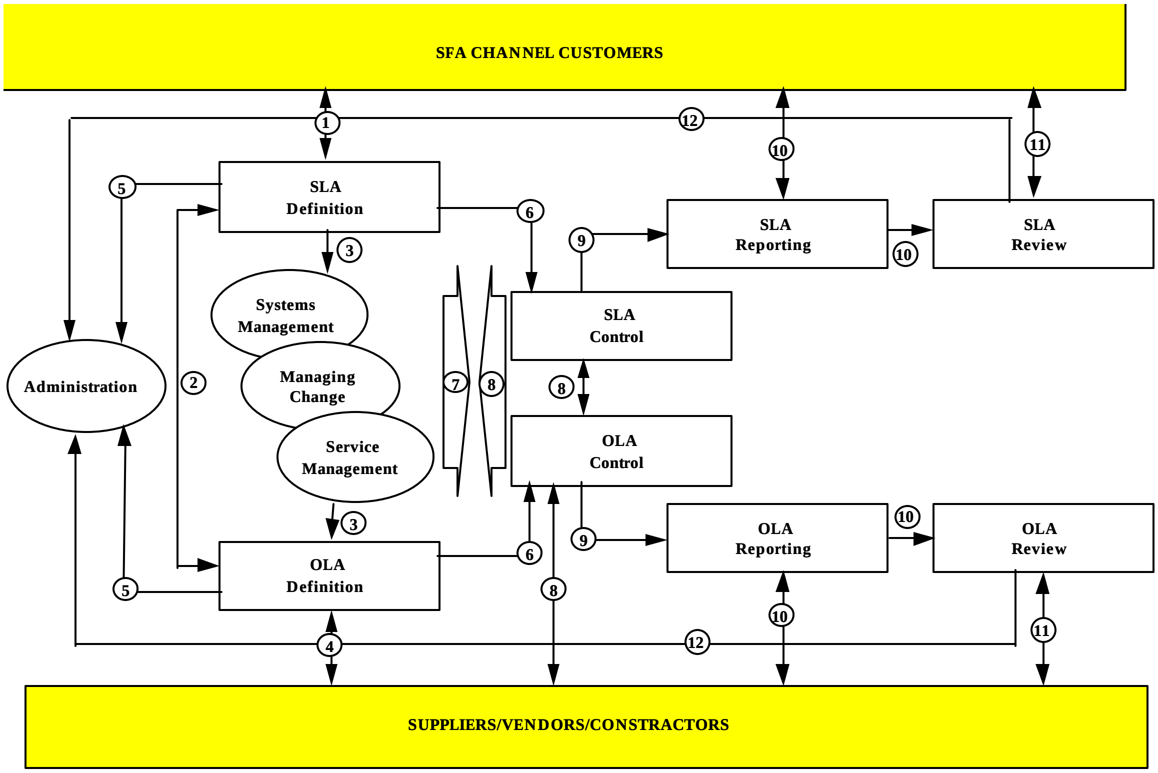


Figure 1. SLA and OLA Management Interfaces

Interface Number	Information	Description
1	Customer Requirements	The process begins with customer requirements, which are received by SLA Definition.
2	OLA Impacts	Any service level requirements which will impact OLAs (i.e., those which are dependent on the service delivered by a supplier) are fed to OLA Definition, so that the SLAs and OLAs can be defined in unison.
3	Operations Architecture Function Impacts	Some service level requirements will have direct impact on other operations architecture functions. These need to be communicated to the service management, systems management or managing change functions, who will then liaison with OLA definition if these requirements are dependent on suppliers. For example, incident resolution targets will be communicated to Help Desk, although actual resolution of incidents will often be dependent on suppliers, and will thus need to be specified in the OLAs.
4	Supplier Impacts	OLA Definition will discuss OLA requirements with suppliers, dependent on the requirements received from SLA Definition and other operation architecture functions.
5	Contractual Input	Once SLAs and OLAs have been agreed to, they will form the main body of contracts held with SFA and its suppliers. These are supplied to administration for ongoing control and maintenance.
6	Defined SLAs and OLAs	The SLAs and OLAs are then passed to SLA Control and OLA Control respectively, for ongoing monitoring.
7	Performance Data	Service Management, Systems Management and Managing Change provide SLA and OLA Control with performance statistics and issues.
8	Performance Issues	SLA Control and OLA Control liaison to discuss performance issues and to identify the cause of any problems. SLA and OLA Control then liaise with the appropriate function or supplier to ensure the issues are resolved as quickly and efficiently as possible.
9	Performance Summaries	Summaries of performance statistics, issues and current status are passed to SLA and OLA Reporting.
10	SLA & OLA Reports	Reports specific to each customer group and supplier are forwarded to these groups and to SLA and OLA Review.
11	SLA & OLA Reviews	Performance against SLAs and OLAs are reviewed between SLA Review and the customers, and OLA Review and the suppliers.
12	Contractual Issues	If amendments are agreed with customers or suppliers, or if performance against SLAs or OLAs may have impact on contractual arrangements, such as incurring financial penalties for under-performing, SLA or OLA Review will pass this information to administration.

The following diagram is a process flow for creating, monitoring, reviewing, and maintaining an SLA. This process will be used to customize the SLA template into an SLA with service levels required for a specific customer.

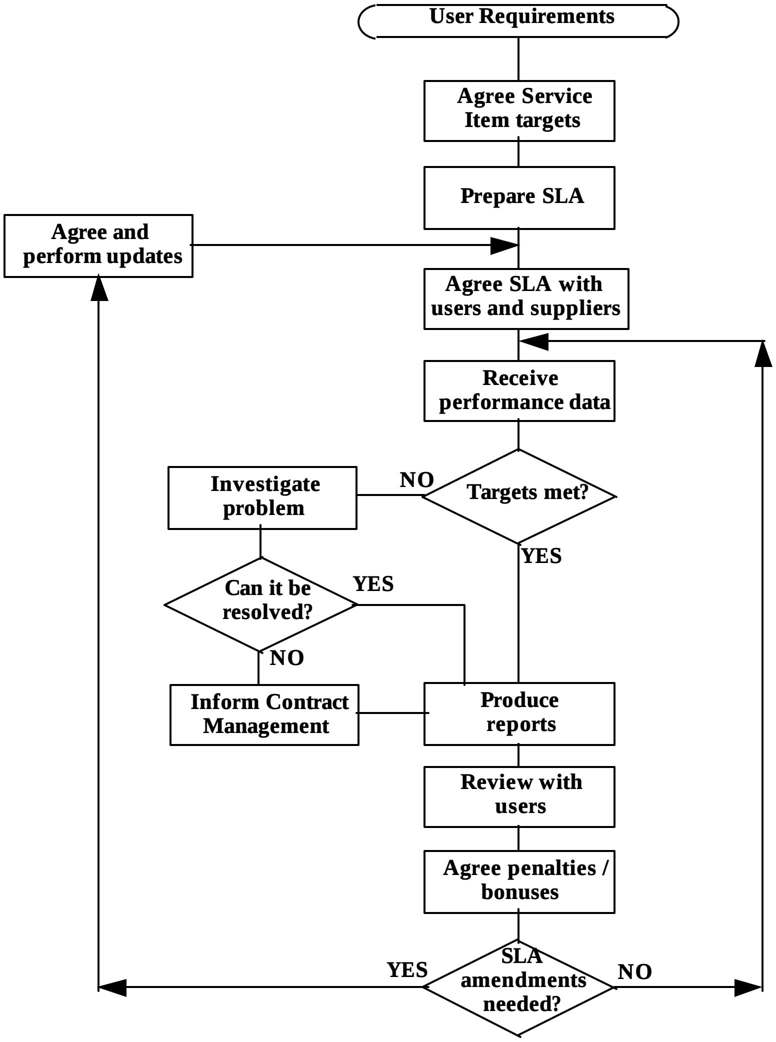


Figure 2. SLA Management Process Flow

It is important also to recognize the lower level processes which need to be defined. These processes should cover the following activities:

- agreeing SLA contents,
- obtaining sign off for an SLA,
- performing an ad hoc query on performance against the SLA,
- collation and presentation of SLA reports,
- performing a review meeting with the customers,
- resolving SLA performance issues,
- re-negotiating SLAs,
- management reporting.

In particular, the process for defining SLAs in more detail is as follows:

- Agree targets for each service item, using the template baseline services as a starting point. It is anticipated that the baseline services denoted in the template will be adequate for the majority of business units. However, where additional services, or extended service levels, are required, the SLA must be customized. The service item goals must be set in conjunction with operational targets.
- Assess resource and cost implications. Whatever targets are agreed, capacity planning, service costing and pricing functions must be involved to assess the resource and cost implications of targets. If customers want high levels of performance from the IT system, they must be made aware of the cost implications, and thus the corresponding effect on chargeback.
- Agree frequency of measurement for each service item.
- Create draft SLA(s), specific to each customer group.
- Obtain sign-off. SLAs must be signed off at the appropriate level, usually by the customer contacts identified, and the head of the IT organization.

4.1.2 Customer Service/Help Desk Interfaces

The functions within Customer Service/Help Desk cannot be considered in isolation. As such, it is important to understand how the independent functions of the Help Desk are related to other functions within this framework. While this information does not present every conceivable interface, it does highlight the major interfaces which need to be considered. The following conceptual diagram depicts the key interfaces that will be addressed:

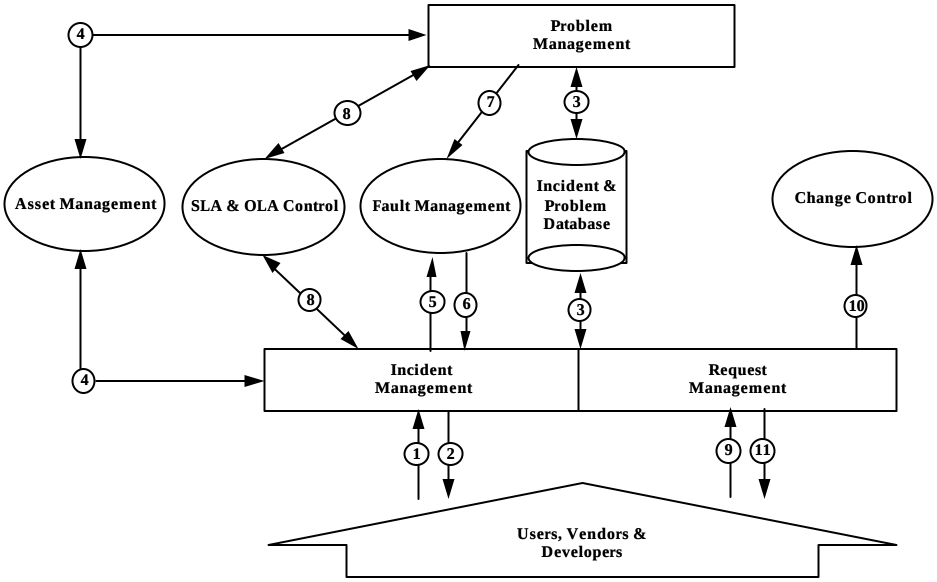


Figure 3. Customer Service Function Interfaces

The following table describes each of the numbered interfaces between the Help Desk functions and other functional groupings in the previous diagram. For each interface, the table below gives the information flowing between functions/functional groupings, and a high level description of the corresponding processes.

Interface Number	Information	Description
1	Call Details	Once a service becomes operational, any incidents experienced by users are raised with Incident Management, and details of the call are logged.
2	Workarounds & Solutions	Incident Management's objective is to resolve the incident and provide immediate feedback to the user, without passing it to other functions for expert resolution. Following implementation of the suggested workaround or solution, resolution of the incident can be confirmed with the user, and the incident can be closed.
3	Incident & Problem Information	Incident and Problem Management use an incident and problem database to hold information related to logging, controlling and closing incidents and problems.

4	Asset Information	Incident and Problem Management also need information from Asset Management (e.g., hardware configuration, software version) to help understand and resolve specific incidents and problems. Liaison with Asset Management is also important to help monitor incident and problem trends affecting particular components.
5	Unresolved Incidents	Incidents which Incident Management is unable to resolve are passed to Fault Management so that a more thorough investigation by technical specialists can take place to resolve the incident. Once an incident has been passed to Fault Management, fault management must resolve it. Incident Management, however, retains the overall ownership of the incident, ensuring that it gets resolved to the user's satisfaction.
6	• Early notification of problems • Workarounds • Resolved Incidents	• If fault management detects negative events, it can then inform Incident Management of the problem, and perhaps an incident workaround, before affected users log a call. Fault management may even log an incident automatically. This enables proactive management of user incidents by incident and problem management. • Fault management also informs incident management of fixes or workarounds to user-raised incidents. Incident management then communicates the fix or workaround to the user, confirms that the incident is resolved, and closes the incident.
7	Problems	Problem management monitors incident trends, looking for evidence of recurring incidents caused by one underlying problem. Fault management attempts to identify a workaround, so that it can be "attached" to the problem, and further occurrences of the incident can be dealt with promptly.
8	Service / Operational Reports	Resolution targets for incidents, problems, etc. will typically be contained within SLAs and OLAs. Incident and problem management will need to provide reports to SLA and OLA management detailing their performance against these service and operational targets.
9	Requests	If users, vendors or developers wish to raise requests relating to the distributed environment, they should do so through the customer service organization. Request management will perform an initial sifting of requests to ensure the same request has not already been raised. It will then log, prioritize, schedule and coordinate the request.
10	Change Requests	If a request requires significant service changes, a change request will be raised with Request management, which will then manage impact analysis and implementation of the request.

11	User Feedback	Users should be kept informed of the status of a request. Satisfactory implementation should be confirmed with the user before the request is closed.

The following diagram represents the process flow for creating, monitoring, reviewing, and maintaining an OLA. This process will be used to customize the OLA template into OLAs that support specific SLAs.

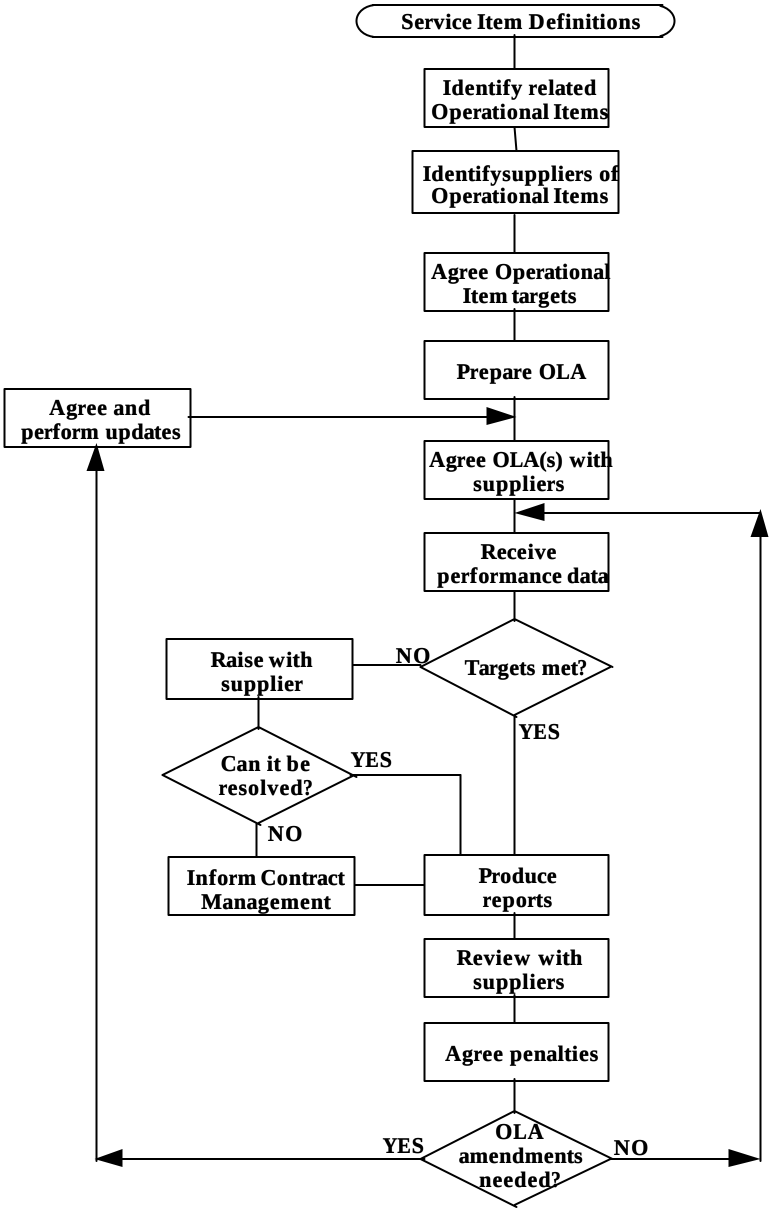


Figure 4. OLA Management Process Flow

It is important also to recognize the lower level processes which need to be defined. These processes should cover the following activities:

- identifying operational items relating to agreed service items,
- identifying suppliers of operational items
- identifying operational items to be included in OLAs
- agreeing OLA contents,

- obtaining sign off for an OLA,
- performing an ad hoc query on performance against the OLA,
- collation and presentation of OLA reports,
- performing a review meeting with suppliers,
- resolving OLA performance issues,
- re-negotiating OLAs,

The lower level process for generating OLAs is as follows:

- Confirm operational items in template. For each service item, assess the constituent operational services which must be supplied to meet that service item goal.
- Assess which operational items will be delivered by suppliers with which formal OLAs are to be created, and which operational items will be measured in internal OLAs. Each different external vendor that provides support should have its own OLA, whereas the internal IT groups can be grouped in a single OLA.
- Assess, and agree with the suppliers, the target level required for each operational item, which will enable the service item target to be met (this must be performed in conjunction with the definition of service item targets).
- Assess resource and cost implications. Whatever targets are agreed, ensure that the resource and cost implications of targets are understood. Suppliers will charge more for aggressive targets, and these added charges will need to be passed on to the customers.
- Agree frequency of measurement for each operational item.
- Create draft OLA(s), specific to each supplier.
- Obtain sign-off. OLAs must be signed off at the appropriate level, usually by the head of the IT organization and the person responsible for delivery of the operational service (IT Services).

Details for the rest of the process flow will be developed later. OLAs will be created with both internal and external suppliers. OLAs with external suppliers will be more formal and may have penalties associated with them. While they are referred to as OLAs, they may in practice be maintenance service contracts. The suppliers may view the OLAs as their own SLAs.